
Edward A. Morse
Vasant Raval

Follow this and additional works at: https://via.library.depaul.edu/bclj

Recommended Citation
Available at: https://via.library.depaul.edu/bclj/vol10/iss2/4

This Article is brought to you for free and open access by the College of Law at Via Sapientiae. It has been accepted for inclusion in DePaul Business and Commercial Law Journal by an authorized editor of Via Sapientiae. For more information, please contact wsulliv6@depaul.edu, c.mcclure@depaul.edu.

Edward A. Morse* & Vasant Raval**

Abstract

A private ordering regime has developed within the payment card industry to define appropriate security practices and to monitor compliance by network participants. Market demands for trustworthy systems upon which consumers and merchants could rely provide incentives for security, which the card brands supplement by privately designed fines and sanctions imposed through contract. Although private ordering has functioned sufficiently well to make payment cards a trusted payment method, the system is not completely secure, as data security breaches continue to occur. This is not surprising, as complete security is not a feasible goal. Nevertheless, some have questioned whether additional government regulation is necessary to protect consumers. This Article explores the effects of legal intervention, including disclosure laws, on this private ordering system. It questions whether additional government intervention would enhance consumer welfare, particularly when consumers will likely bear the ultimate costs of such regulation. It recommends modifications in breach disclosure laws to eliminate individual notice requirements in favor of public notices, which may reduce costs and enhance consumer welfare. It challenges “bounty” enforcement regimes, such as FACTA, which offer little marginal benefit to consumers while substantially raising costs. It identifies practical and political problems presented by the different capacities of large and small firms to bear security costs, which are not easily solved under either private ordering or legislative approaches. Finally, it offers a set of policy issues as a possible agenda for consideration by policy makers and researchers in this domain.

* Professor of Law, McGrath North Mullin & Kratz Endowed Chair in Business Law, Creighton University School of Law.
** Professor of Accounting, Creighton University College of Business Administration. The authors are grateful for comments and insights on an earlier version of this paper from participants at Economic Governance and Competition: The Pros and Cons of Private Ordering in the Shadow of the Law, held at Tilburg University, The Netherlands.
Private ordering describes a broad range of methodologies for governing behavior and resolving disputes that depart from a model of governance by law promulgated by sovereign governments and enforced through government-sanctioned courts. Although private ordering can occur in contexts that are effectively insulated from the reach of traditional law enforcement, it often occurs within the public legal system. This close relationship between public and private
Realms causes private ordering to occur, as some have described it, within the "shadow of the law."  

Private ordering literature often focuses on situations that are rooted in contract, where self-interested behavior moves the parties toward privatizing the rules that govern their relationship and the processes for resolving disputes and enforcing their agreements. This often works well for groups with particularized needs, which are not well served by the traditional legal infrastructure.  

But other instances of private ordering are more systematic and perhaps more closely connected to the legal order. For example, private entities in the United States promulgate generally accepted accounting principles (GAAP). These principles and standards have become the established basis for U.S. financial reporting, and they are also used for limited purposes in constructing federal income tax laws. In this context, private ordering may be considered as a conventionally outsourced infrastructure, on which the law depends heavily. Just as a firm chooses to outsource a function based on efficiency considerations, governments also outsource the machinery of regulation, choosing in some cases to leave matters of rulemaking and enforcement outside of government hands. 

Public interests may also be implicated when private ordering occurs, causing government to intervene in order to protect those interests. In some cases, mere threats of government intervention may induce self-regulation efforts designed to preempt government action,
thereby preserving private autonomy.\(^8\) In this sense, law may be seen as a light that shines on private behavior, causing self-correction without the need for government displacement of the private benefits obtained from autonomous coordination, such as "insourcing" rulemaking and enforcement functions.\(^9\)

Whether law casts a shadow or shines a light, government policymakers should fully comprehend how private ordering works today before choosing to intervene. A careful consideration of all options in the range of private ordering and public regulation is critical to achieve pre-set objectives in a cost-effective manner. While insourcing is an option often exercised, in some situations, a complete takeover of standard-setting and enforcement machinery proves not only costly, but also dysfunctional for the industry and its stakeholders.

This Article addresses the respective roles of private ordering and public laws in the development and implementation of the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS have emerged from collective actions by payment card networks, and they are rooted in the economic self-interests of network participants to achieve a trustworthy means of channeling electronic payments. Protections for consumers can thus be viewed as an intentional byproduct of this self-interested behavior. Public laws have influenced the development of these standards, but have done so with minimal interference. However, threats of additional government intervention loom in the context of significant security failures within the industry. Whether intervention is appropriate or desirable, as well as the extent of that intervention, presents some troubling economic and political questions, which are explored below.

\(^8\) See id. at 428.
\(^9\) The PCAOB may be viewed as an example of such displacement:

Congress created the Public Company Accounting Oversight Board (the PCAOB or the Board) in direct response to the collapses of Enron and WorldCom, and the bevy of other accounting and corporate governance scandals capturing front page headlines in 2001 and 2002. As the cornerstone of the Sarbanes-Oxley Act, its immediate mission was to restore public confidence in the securities markets by ensuring the integrity of the accounting firms that audit financial statements for publicly traded companies. To achieve this end, Congress vested the PCAOB with broad governmental powers and responsibilities, including the authority to register accounting firms that audit public companies; enact rules setting standards for auditing, quality control, ethics, and independence; inspect on a yearly basis the nation's largest accounting firms and inspect other firms at least once every three years; investigate accounting firms and their associated persons for possible violations of PCAOB rules or the federal securities laws; and impose discipline for established violations through a range of sanctions including censures, temporary suspensions, permanent bars, and substantial monetary fines. The PCAOB is now, without question, the congressionally designated auditor for auditors. Nagy, supra note 5, at 977–78 (footnotes omitted).
We argue that the robust competitive market forces in the credit card industry, coupled with a dynamic technological environment, counsel against government intervention regarding the standards for security or the consequences of unsecure behavior. Consumers will likely bear the additional costs of intervention, and it is far from clear that moving the locus of enforcement from the network to the government or deepening compliance burdens would provide net marginal benefits in this context without significantly disrupting the payment card ecosystem, particularly when that system includes small merchants who cannot effectively spread their compliance costs. However, should legislators mandate constructive and equitable \textit{post hoc} procedures for disclosing security failures, these procedures may enhance the effectiveness of market forces in achieving greater consumer protection.

We also discuss the possibility that ancillary externalized costs, including the costs imposed on issuing banks to replace cards that have been compromised, are not adequately addressed by contract within the private ordering regime. Although the marketplace is capable of allocating these costs (and probably routes them back to consumers), choosing to reallocate by creating new legal paths for recovery presents a political choice, rather than economic choice, that is unlikely to enhance consumer welfare to any significant extent.

Part I provides a brief overview of private ordering concepts and identifies some situations in which private ordering functions displace, and are sometimes displaced by, regulatory intervention. Part II addresses the structure of the payment card industry and a summary of critical incentives favoring security among those who participate in the payment card network, as well as identifying some limitations in those incentive structures that may result in externalized costs. Part III examines the current state of data security standards (PCI DSS) and enforcement of those standards using private ordering principles. Part IV assesses several incursions into this private ordering regime, including legal requirements for disclosure when breaches occur, generalized sanctions by the Federal Trade Commission (FTC) for unsecure behavior, and attempts to create new legal pathways for reallocating breach-related costs within the network. Part V summarizes research and policy issues and concludes with observations about government intervention in this dynamic technological environment.

\section{I. Private Ordering in a Public Context}

Private ordering occurs ubiquitously in market economies in which individuals and firms have incentives to optimize their respective ben-
benefits from yet unregulated or emerging economic relationships. Within the realm of contract, parties negotiate to achieve mutual benefits through exchanges, which generally may be tailored freely to address their particular needs and expectations. At its most basic level, law provides a basis for transactional security, which confirms that expectations reflected in an executory agreement will indeed be fulfilled.\(^\text{10}\)

Law may also intervene to affect the content of private agreements by constraining the terms for agreement, thereby reflecting communal norms for expected behavior instead of leaving such matters to private negotiation. Doctrines of good faith and unconscionability are examples of this form of intervention.\(^\text{11}\) In this way, law defines the outer limits of private ordering, providing a boundary that channels behavior toward desirable ends and away from undesirable ones, while preserving autonomous decision-making as the primary mechanism for governing behavior.

Constraints are often imposed when private ordering fails to produce socially desirable outcomes. For example, concerns about disparities in bargaining power and the economic necessity of formal contracts in consumer transactions have provided the basis for legislation injecting \textit{ex ante} restrictions into agreements for the stated purpose of protecting consumer interests.\(^\text{12}\) Political concerns about the public consequences when private ordering fails may also trigger some additional government involvement in the private regime.\(^\text{13}\) However, regulators must possess considerable knowledge of the economic relationships within an industry in order to draft effective rules. Govern-

\(^{10}\) See, e.g., John O. Haley, \textit{Why Study Japanese Law?}, 58 AM. J. COMP. L. 1, 3 (2010) ("Few indeed dispute that wealth-generating activity requires sufficient political stability and a social environment in which individuals acting with others are willing and able to invest effort and assets in anticipation of economic gain. Political stability is a necessary but insufficient condition. Equally necessary are transactional security and assurance that future returns will not be confiscated, i.e., protection of contract and property. Confidence in legal recognition and protection of property encourages investment in wealth-generating enterprises. Similar assurance of legal enforcement of contracts in turn fosters exchange and transactions among strangers. These features taken together, the argument goes, help to explain why economic activity appears to flourish best in stable political orders in which private law systems function.").


\(^{13}\) See Nagy, supra note 5, at 977–78; see also Schwarz, supra note 1, at 347 ("Where public confidence in the legitimacy of a privately ordered scheme is shaken, governmental delegation should be scrutinized to determine whether it can make the private ordering more efficient.") (second emphasis added).
ment regulators must either develop this knowledge internally, or they can rely on other sources for that expertise, effectively co-opting rules or standards developed through private ordering and converting them into public laws.\textsuperscript{14} Courts, in particular, may rely on practices and customs in interpreting rules in commercial settings, reflecting the philosophy of Karl Llewellyn that the law must reflect commercial realities.\textsuperscript{15}

Alternatively, in lieu of specific rules, government may also use more generalized approaches, which require discretionary intervention to constrain behaviors that may be undesirable or unfair, such as the FTC's pursuit of "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."\textsuperscript{16} Such an approach allows government power to respond to the most egregious cases of behavior which might otherwise not fall within existing legal regimes, while at the same time allowing rules to develop over time, taking into account changed circumstances and conditions. However, these approaches also present risks associated with discretionary justice, where the expected certainty and predictability—hallmarks of the rule of law—may compromise the interests of those being regulated.\textsuperscript{17}

In addition to substantive rules, the process for resolving disputes may also leave room for private ordering. Lawsuits provide a public means to call attention to allegations of behavior that breaches legal norms.\textsuperscript{18} In this sense, they serve important functions that may im-

\textsuperscript{14} See, e.g., Cunningham, supra note 5, at 313 ("PCAOB began its mission by adopting a substantial body of GAAS promulgated by the AICPA.").


\textsuperscript{17} See Belt, supra note 16, at 4–5. In 1994, Congress enacted 15 U.S.C. § 45(n), which denies the Commission authority to declare a practice as unfair "unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." \textit{Id.} at 4 (quoting 15 U.S.C. § 45(n)). Although this may provide a constraint on administrative power, such balancing still entails considerable uncertainty for those affected. See \textit{id.} at 5. See also Edward A. Morse, Reflections on the Rule of Law and "Clear Reflection of Income": What Constrains Discretion?, 8 CORNELL J.L. & PUB. POL'Y 445, 461 (1999) ("[D]esirability of rule-based decisionmaking depends in part on which is trusted (or feared) most: government decisionmakers (with the potential to violate individual rights through discretion) or citizens (with the potential to exploit weakness in rules to the detriment of the common good.").

\textsuperscript{18} See Haley, supra note 10, at 5 (noting that "a lawsuit may function more as a public signal of untrustworthiness than as a legal remedy").
prove the quality of law itself. However, many lawsuits are settled under terms that preclude disclosure, reflecting a preference for private ordering over public justice. To some extent, this may reflect concerns about losing control of the outcome to a disinterested third party, as well as other prudential factors affecting risk management.

Thus, the dispute resolution process may also be privatized—indeed, this has become a common provision in contractual arrangements. Scholars have identified several reasons for these practices. Private dispute resolution may achieve timeliness that overburdened public forums cannot deliver. It may also provide decision-makers with particular expertise in these kinds of disputes, which may not be readily available in the hands of generalist judges.

In international contexts, private dispute resolution also solves the problem of sovereignty claims from competing jurisdictions, and in this way serves the needs of parties whose activities transcend geographic borders. Such transcendence may not be complete, to the extent that legal regimes may indeed be invoked by a dissatisfied party. Nevertheless, the promise of private ordering in this regard has been realized considerably in matters of international trade. Moreover, as discussed below, this feature of private ordering also has promise in the realm of payment systems, which often span geographic borders.


20. See, e.g., Ronald Lee Gilman, Resolving Commercial Cases through Alternative Dispute Resolution, 26 U. Mem. L. Rev. 1121, 1124 (1996); David J. McLean & Sean-Patrick Wilson, Compelling Mediation in the Context of Med-Arb Agreements, 63 Disp. Res. J. 28 (2008) (“In most situations, it is in the best interest of the parties to amicably resolve their disputes during the mediation step and avoid the cost of arbitration and losing control over the outcome of their case.”).


22. See, e.g., Murray, supra note 19, at 152 (noting “rapid finality” as a claimed advantage of arbitration).

23. See, e.g., Chris Guthrie, Misjudging, 7 Nev. L.J. 420, 454 (2007) (“[T]here is reason to believe that disputants seeking an accurate outcome might fare better in arbitration, particularly where the arbitration involves a diverse panel of subject-matter experts.”).

24. See Drahozal, supra note 1, at 1037 (discussing “Law Merchant” concepts in international arbitration). It should be noted, however, that Drahozal also concludes that national law is still used widely in international arbitration panels. Id. at 1038–39.

25. See id. at 1040 (noting that public courts play an important role in enforcement).
PRIVATE ORDERING AND PAYMENT CARD SECURITY

II. SECURITY, SANCTIONS, AND SELF-INTEREST IN THE PAYMENT CARD INDUSTRY: AN OVERVIEW

Private ordering has played a crucial and ongoing role in the development of payment cards as a significant mechanism for payment. Private systems of regulation have developed to induce consumers' and merchants' trust and confidence in transacting payments through these networks, with only minimal interference in matters of data security. As discussed below, self-interested behavior has induced commercial participants to join together in creating a trustworthy environment.

The payment card industry provides a valuable intermediary service between consumers (cardholders) and the merchants who accept cards for payment (merchants).26 Although variations in the structure for delivering and marketing payment card services occur within the industry,27 the principal relationships within the network are illustrated in Figure 1, below.28

Trustworthiness is critical for participation in both the merchant and consumer markets for payment card services. Merchants require assurance that they will receive payment for their goods and services. Consumers require assurance that merchants will accept this form of payment and that they are liable only for authorized charges. By providing this assurance, immense benefits occur within the economy for participants. For example, consumers and merchants alike avoid security and transaction costs associated with cash; they also benefit from reduced transaction costs for credit, which likely generate additional completed transactions. The network of trust relationships inherent in the industry is illustrated in Figure 2, below, An Anatomy of PCI DSS.

The sheer volume of card-based transactions in the United States—more than three trillion dollars in 2009—speaks to their utility.29 Although economically difficult to assess the independent value created by this payment medium, commentators have estimated that if it ap-

---

28. See id. at 542.
proaches even a modest five percent of this three trillion dollar volume ($150 billion), it will far exceed the total costs incurred from such ancillary consequences as identity theft. Alternatively, market value associated with card brands also shows their economic significance, as the combined market capitalization for the four largest firms, American Express, Discover, MasterCard, and Visa, totaled more than $180 billion in April 2010. Indeed, the payment card industry has earned its own economic identity within financial services, and those in charge of its governance should be justifiably concerned about the protection of its market capitalization.


The assurance that consumers require for participation comes primarily from contract. In order to induce consumer trust, card issuers have aggressively promoted consumer protection from fraudulent transactions, offering zero liability for transactions within the network.\footnote{See, e.g., Zero Liability for Lost and Stolen Cards, MasterCard, http://www.mastercard.us/zero-liability.html (last visited Jan. 11, 2012) [hereinafter Master Card Liability]; Visa Security Program, Visa, http://usa.visa.com/personal/security/visa_security_program/zero_liability.html (last visited Jan. 11, 2012).} Congress has enacted federal laws to require that consumers bear no more than fifty dollars in liability for fraudulent transactions,\footnote{See Truth in Lending Act, 15 U.S.C. § 1643(a)(1) (2006) (limiting cardholder liability for unauthorized credit card charges to $50); Electronic Funds Transfer Act, 15 U.S.C. § 1693g(a) (2006) (limiting consumer losses for debit cards).} but the fact that payment card firms offer consumers more than is federally mandated under these laws suggests that competition for customers drives the industry to act in favor of consumer well-
being. Self-interest produces this result: if consumer fears regarding unauthorized charges induce them not to use their cards, the payment card industry makes no profits.

Fraudulent transactions do occur, and these transactions impose costs within the payment card network. When lost or stolen card information is used, someone other than the legitimate cardholder must bear the loss. Typically this cost is borne by the merchant who accepts the card for payment. When a customer disputes a charge, the bank issuing the card (with whom the consumer has a contractual relationship) reverses the charge and notifies the merchant's bank (sometimes known as the acquiring bank) to return the funds pending the resolution of the dispute. Absent a signed sales receipt from the cardholder, the merchant is likely to bear the loss. The merchant's bank (or "acquiring bank") has two incentives to pass this cost along to the merchant: (1) a short term incentive to avoid the immediate cost of the charge-back, and (2) a long-term incentive to reduce the risks of fraudulent behavior generally by incentivizing the merchants to engage in proactive behavior. Merchants, in turn, will likely pass these costs along to their customers, although competitive conditions may constrain their ability to do so.

Some fraud within the payment card industry can be attributed to the fault of consumers who lose cards or related information through their own unsecure behavior. For example, fraudulent email requests (also known as "phishing attacks") have proven remarkably successful in extracting data directly from consumers based on mistaken beliefs about the nature of the disclosure. However, protections offered to consumers in the United States are generally independent of consumer fault, so long as they occur within the network. In this sense,

34. It is curious that this phenomenon has been limited to the U.S. See Visa Security Program, supra note 32, (noting that the zero liability policy "covers U.S.-issued cards only"). It is possible that legally-imposed low liability limit may be responsible for nudging card issuers toward competing in a manner that favored consumers.

35. See generally Paycom Billing Servs., Inc. v. Mastercard Int'l, Inc., 467 F.3d 283, 286–88 (2d Cir. 2006). Losses may be particularly acute in so-called "card not present" transactions, including transactions over the Internet. See also Morse & Raval, supra note 27, at 543.

36. See Morse & Raval, supra note 27, at 543. However, in some cases competitive conditions to attract merchants may cause some banks to absorb these charges instead of passing them back to their customers, though this is likely to be rare. Id. at n.36.

37. See id. at 544.


39. However, the MasterCard policy includes a caveat that the customer must have "exercised reasonable care in safeguarding your card from any unauthorized use," which means "you did not provide, directly, by implication or otherwise, the right to use your card and you received no benefit from the 'unauthorized' purchase." See Master Card Liability, supra note 32. Presuma-
the framework for consumer protection departs from common law standards of negligence, which traditionally reallocate losses based on fault. However, the merchant community, which generally bears the initial loss in these circumstances, may be a “superior risk bearer” if not the “least-cost risk avoider” in the sense that merchants are able to protect themselves to some extent through security measures. If a loss does occur, the merchant community can spread the cost more effectively than an individual consumer. Nevertheless, some merchants permit credit card payments without signatures or identification on small transactions, presumably reflecting a business decision that the benefits of speedy transactions are more important than marginal protections against chargebacks from capturing a signature. Thus, merchants self-select cost spreading as a means of response. Others accepting payments via the Internet are effectively forced to accept payments without a signature, and presumably the competitive conditions within this market allow them to engage in cost shifting for the fraudulent charges they are likely to incur, although competition with “brick and mortar” businesses not subject to these constraints will presumably provide a limit on such shifting.

Other fraud cases result from the unsecure behavior of merchants, processors, or other participants within the payment card network, which permits hackers to obtain payment card data and perhaps other personal information without the consumer’s consent. Hackers have accessed data from merchants in notorious cases (such as Hannaford Grocery, TJ Maxx, and others) generating large scale instances of card fraud. According to one source, hackers supposedly gathered information from the TJ Maxx network for nearly two years before using those accounts for fraudulent purposes, suggesting that criminals approach this activity scientifically in the manner of a business, rather than as a random act of theft. Criminals routinely trade credit card information for amounts ranging from $.10 to $25.00 per card number,
with one study estimating the total potential worth of credit cards sold illicitly at $5.3 billion.\textsuperscript{43}

An unsecure merchant who inadvertently discloses the card information presents a risk that such information may be used to commit fraud at other merchants. As long as this fraud occurs in transactions with other merchants within the payment card network, the cardholder is protected from direct liability. However, by increasing the vulnerability to fraud within the network, this unsecure behavior potentially generates externalized costs for other merchants. Asymmetries may occur between the unsecure behavior and the additional fraud risks exported to others. For example:

- Merchants that impose strict security measures on card users, such as a robust authentication requirement, are less likely to be targets for fraudulent behavior due to the threat of detection. In contrast, merchants that rely on "card not present" transactions or who dispense with signatures due to transaction volume considerations face comparatively more risk.

- Merchants that sell products or services that can be cancelled when the fraud is discovered (e.g., tuition for an academic degree or warranty services that can be discontinued), would incur limited economic losses from fraud, as compared with those who cannot retract or cancel a transaction \textit{post hoc}.

- Merchants that sell goods or services with insignificant marginal costs (e.g., books or music delivered electronically) would face comparatively limited (out-of-pocket) economic consequences for fraud in comparison with others who provide tangible goods or services with significant marginal costs.

The payment card network provides additional incentives through private ordering, which potentially correct these asymmetries between the individualized assessments of costs and benefits for particular merchants. As discussed in greater detail below, the network provides the standards for expected security behavior; private firms, accredited through private ordering, provide compliance monitoring; and breaches are punished through fines imposed within the network.\textsuperscript{44}

These measures to enhance security throughout the network are rooted in shared incentives for broader payment card usage and pro-


\textsuperscript{44} Since these fines are imposed privately, their frequency and volume are not entirely known, making their particular effectiveness difficult to evaluate. See Sasha Romanosky & Alessandro Acquisti, \textit{Privacy Costs and Personal Data Protection: Economic and Legal Perspectives}, 24 \textit{Berkeley Tech. L.J.} 1061, 1077-78 (2009).
tection of the card brand’s reputation. As VISA has admitted in a Form 10K filed with the Securities Exchange Commission (SEC), payment card breaches affect its reputation and profitability:

We, our customers, merchants and other third parties store cardholder account information in connection with our payment cards. In addition, our customers may use third-party processors to process transactions generated by cards carrying our brands. Breach of the systems on which sensitive cardholder data and account information are stored could lead to fraudulent activity involving our cards, reputational damage and claims against us. If we are sued in connection with any data security breach, we could be involved in protracted litigation. If unsuccessful in defending such lawsuits, we may be forced to pay damages and/or change our business practices or pricing structure, any of which could have a material adverse effect on our revenues and profitability. In addition, any reputational damage resulting from an account data breach at one or more of our customers, merchants or other third parties could decrease the use and acceptance of our cards, which could have a material adverse impact on our payments volume, revenues and future growth prospects. Finally, any data security breach could result in additional regulation, which could materially increase our costs.\textsuperscript{45}

MasterCard has made similar disclosures, which also emphasize the reputational costs and adverse impacts on transaction volumes from increased fraud claims.\textsuperscript{46}

The above disclosures also indicate that costs imposed within the network are not the only potential costs from a security breach. Banks issuing payment cards may experience particularized costs associated with cancelling compromised cards and reissuing new ones.\textsuperscript{47}

Moreover, consumers affected by identity theft may experience losses outside the scope of the payment card network, so that the zero liabil-

\textsuperscript{45} Visa, Inc., Annual Report (Form 10-K) 25–26 (Nov. 20, 2009).

\textsuperscript{46} MasterCard, Inc., Annual Report (Form 10-K) 39 (Feb. 18, 2010):

[A]ny damage to our reputation or that of our brands resulting from an account data breach could decrease the use and acceptance of our cards, which in turn could have a material adverse impact on our transaction volumes, revenue and future growth prospects, or increase our costs by leading to additional regulatory burdens being imposed upon us.

. . . Increased fraud levels involving our cards could lead to regulatory intervention, such as mandatory card re-issuance, adoption of new technologies or enhanced security requirements, and damage to our reputation and financial damage to our brands, which could reduce the use and acceptance of our cards or increase our compliance costs, and thereby have a material adverse impact on our business.

\textsuperscript{47} See, e.g., TJX, Financial Institution Plaintiffs Settle Claims in Breach of 46 Million Credit Cards, 14 BNA ELEC. COMMERCE & L. REP. 1296 (2009) (discussing settlements in litigation against merchant with payment card security breach, including substantial amounts to banks required to issue new cards for those compromised by disclosure).
ity protections applicable to unauthorized charges may not effectively make them whole.\textsuperscript{48}

For the entire ecosystem and its participants, it is important to recognize that empirical evidence indicates that data breaches have resulted in significant abnormal negative stock market returns in the immediate and medium-term (one to two years) time horizons following a firm's announcement of a breach.\textsuperscript{49} If investors punish an insecure firm, recovery from such losses in market capitalization may take a long time. This market reaction may provide an additional incentive for security.

Whether regulated or private-ordered, protection from data breaches is, and will remain, a key imperative in this industry. However, the content of the security standards and the nature of enforcement measures utilized to ensure compliance within the industry remain mostly within the realm of private ordering. Significant aspects of the private ordering regime of PCI DSS are discussed in Part III, below, and significant legal incursions into that regime are explored in Part IV.

III. PCI DSS: Private Ordering of Security

In this section, we discuss first the role of DSS in PCI. We contend that DSS are an infrastructure in itself, providing multidimensional, global support to the entire domain space. Second, we examine an anatomy of the PCI DSS, which suggests significant bonding of security as a system embedded within the PCI. Then we look at the strategic goal of the PCI, via DSS, to maintain reputation through established and ongoing trust in the system as a whole. We argue that the security measures are designed only to achieve stable trust levels; that is, security is not the ultimate objective, trust is. DSS have emerged cooperatively as a socioeconomic system that is highly dependent on technology, and that dependence suggests a continuing

\textsuperscript{48} See Synovate, Federal Trade Commission - 2006 Identity Theft Survey Report 3–6 (2007), http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (estimating the median costs incurred in connection with frauds committed by opening new accounts as forty dollars per consumer and the median value of goods and services obtained by thieves in this context was $1,350). However, the report also notes that consumers are unlikely to bear fraud costs directly due to legal protections operating in their favor. See id. at 6, n.5.

\textsuperscript{49} See Edward A. Morse, Vasant Raval, & John R. Wingender, Jr., Market Price Effects of Data Security Breaches, 20 Inf. Sec. J. 263 (2011). While these results held true for breaches affecting a database of public companies, they did not hold true among all subcategories of this database. Id. Stock prices for financial services and industrial firms were both affected, but retailers were apparently not affected. See id. at 269-72. Further, responses may also vary based on the type of breach. Hacking generated no significant impact, but stolen laptops or other fraudulent access generated more significant results. See id.
role for cooperative standard setting for the foreseeable future. A schematic showing the private ordering construct built into the PCI is shown in Figure 3, below.

Figure 3. The Private Ordering Construct in the PCI

A. DSS in PCI: A Brief History

Five card brands: American Express, Visa, Master Card, Discover, and JCB worked together to release Data Security Standards on December 15, 2004. Prior to launching this cooperative venture, each card brand followed its own security "standard" in contractual relationships with entities within its network. PCI DSS as a unified framework aimed to improve coordination across entities involved, harmonize expectations, and improve efficiency through shared security expertise. However, that coordination could also tend to reduce interbrand competition over security features.50

50. Collusion on matters regarding security would be expected to generate consumer welfare if the outcomes resulted in fewer fraud claims than under a competitive regime. The oligopolistic nature of card brand cooperation here may present antitrust concerns (which are avoided under U.S. law to the extent that cooperative behavior is the product of regulation, rather than private ordering), but they are beyond the scope of this article. For additional discussion, see Barak D. Richman, The Antitrust of Reputation Mechanisms: Institutional Economics and Concerted Refusals to Deal, 95 Va. L. Rev. 325, 327 (2009).
The PCI DSS framework is organized into a set of twelve related “requirements” further classified into over 300 sub-requirements in its current version. Non-linear in nature, each of these applies at a different level; for example, network level, communication level, and application level. The original security framework announced in December 2004 (Version 1.0) was revised in September 2006 (Version 1.1) to provide clarification to Version 1.0 and incorporate minor revisions. Released in October 2008, Version 1.2 replaced Version 1.1 effective 2009; however, this new version did not change any of the requirements. Rather, it improved clarity, accommodated greater flexibility in compliance modes, and addressed evolving risks and threats, including issues involving wireless networks deployed for payment processing. In August 2009, the revised version 1.2.1 was announced, primarily to effect minor corrections and improve consistency between the requirements and supporting documents.

The PCI Data Security Council (PCI DSC) launched a revised version of the standards, V2, in October 2010. Contrary to expectations, this much anticipated pronouncement did not change much. Numerous revisions were in the spirit of clarification, to ensure that concise wording portrayed the desired requirements. For example, several clarifications addressed the timing, extent, or documentation of testing procedures. Comparatively few revisions substantively modified compliance obligations. For example, V2 provided more examples of risk assessment methodologies. A third category of revisions, called Evolving Requirements (formerly, Enhancements) included changes to ensure that the DSS are up to date with emerging threats and changes in the market. Only one Evolving Requirement was present in V2, making it obligatory to (1) rank identified vulnerabilities according to risk, and (2) test the procedure to address high-risk vulnerabilities. The Council noted that this evolving requirement of identification and ranking of high risk vulnerabilities is considered a best practice. This remains a best practice until June 30, 2012, after which it becomes a requirement.51

The payment card industry today is a thriving business, with combined market capitalization for the four largest firms, American Express, Discover, MasterCard, and Visa, totaling more than $180 billion.52 MasterCard, the first of these firms to issue stock to the public, recently sold for nearly five times the IPO price from only four

52. See Evans, supra note 31.
years ago—a testament to the market’s assessment of the promise for growth inherent in these enterprises.

The role of PCI DSS seems central to this growth, as the perception of security represents an inherent characteristic of an effective payment system. In this regard, private ordering tends to follow logical boundaries, not legal ones. Implementation spans global networks that transcend national boundaries, requiring the emergence of a sophisticated infrastructure. Specification of security requirements, interpretation of standards and implementation within particular systems, and the testing and certification of such systems for compliance, have generated a large and growing economy within the industry. A network of qualified private firms has emerged, which are devoted to assisting organizations with implementation of the DSS and to certify continued compliance for the benefit of the network. Figure 4, below, illustrates in some detail the various relationships within the DSS infrastructure.

While such elaborate and impressive infrastructure and attendant ecosystem is impressive in all aspects, advocates of regulation who wish to not rely on this extralegal mechanism may have cause for concern. For example, the requirements are set by the PCI DSC, but responsibility for managing the PCI DSS compliance program has been given to the acquirers and acquiring banks, which contract with their respective merchants. While this may make logical and practical sense (due to privity of contract), acquirers may not fully implement compliance burdens to the extent that they conflict with the acquirers’ interest to generate fees from those same merchants. An additional concern exists with the certification process embedded within the PCI DSS infrastructure. The common control of certification and training of assessors may generate conflict of interest issues to the extent that the same entity performs standard-setting and certification responsibilities.

53. See id.
54. For example, Visa publishes and maintains a “Global List of PCI DSS Validated Service Providers” (as of 5/5/2010) that lists firms who have validated compliance with PCI DSS, along with the Qualified Security Assessor (QSA) responsible for the firm certification. See Visa’s Global Registry of Service Providers, VISA (Oct. 13, 2010), http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf.
56. For example, size-based constraints may represent a practical economic consideration that balances the desirability of access to the network against the compliance burdens that could limit participation by smaller firms. See infra note 62.
B. Maintaining Trust within the PCI

The PCI Security Standards Council affirms that it set DSS with a view to provide technical and operational requirements to protect cardholder data.\textsuperscript{57} The SSC does not refer to the establishment of marketwide trust across stakeholders as an overall intent of the standards, but this is understandable. A notion of trust is a behavioral

phenomenon, involving the psyche of participants across the industry.\textsuperscript{58} Trust is affected by cost-benefit considerations, in which economic benefits from a convenient payment option are balanced against the costs allocated to participants. The DSS framework provides an important contribution through attempting to outline broad security requirements, which facilitate trust. But when these security requirements fail, trust can also be buttressed by other industry practices, such as assurances limiting consumer liability. In this regard, one might surmise that the industry attempts to keep its infrastructure in balance so that consumer trust is preserved even when occasional data security breaches actually occur.

Covered entities may fall out of compliance at any time. Implementation of PCI DSS does not necessarily preclude data security compromises. New threats to emerging vulnerabilities will continue to surface. An entity otherwise compliant with PCI DSS may not have yet addressed changes within the security environment, including the evolving capabilities of criminals to circumvent controls. Therefore, it is only superficial to think of the aim of PCI DSS as a bulletproof security framework. Nevertheless, failures draw claims for a review of the extralegal mechanisms operating within the PCI DSS to ensure that affected parties are treated fairly.

\subsection*{C. Life-Cycle Stages of PCI and Their Relation to DSS Technology and Innovation}

The private ordering system within PCI is embedded within a socio-technical system that governs the market and drives its behavior. The payment card—or its logical equivalent—is the key to its operation. In turn, the accompanying information technology provides transactional assurance. The only thing constant about such technology is change, which makes security a moving target. Securing cardholder data was much easier in a relatively closed system with a well-defined perimeter and known exit and entry points, which existed prior to the Internet. However, systems now interface generally with a world of

\textsuperscript{58} See Vasant Raval & Ashok Fichadia, \textit{Risks, Controls, and Security} 154–55 (Wiley 2007). As Raval and Fichadia observe,

\begin{quote}
\textit{[S]ecurity is an either-or proposition. [S]ome system, software, or process is either secured or not secured. On the other hand, degrees of trustworthiness can be defined and used. The source of security is the presenter, who can claim to be secured or not secured, whereas trust is a property of the sender, who makes implicit claims for wanting to be trusted. Products, processes or systems can be claimed to be secured (or not secured); in contrast, evidence and analysis can lead to judgment as to trustworthiness of such objects or entities.}
\end{quote}

\textit{Id.} at 154–55.
loosely connected, largely unsecure, networks. The introduction of wireless networks presented new risks, which did not exist in hardwired systems. As cloud computing practices emerge, moving the locus of data from the source to third-parties and public clouds, additional players in the PCI domain may bear responsibility for security, adding to the complexity in this environment.59

Thus the industry faces an essential challenge of addressing security needs in this dynamic environment. The PCI Data Security Council is currently charged with the task of promulgating standards that take into account this technological dynamism. As shown in Figures 3 and 4, above, PCI DSS include structure, process, and information (i.e., the standards). Although cooperative rulemaking is readily seen in the development of the industry-wide standards, structures and processes for implementation are generally handled by the brands independently (see Figure 4). These also reflect the imprint of private coordination and development within each brand network, with the potential for variation among the card brands.

This current stage of cooperative security development in standard design could change in the event that a payment card brand independently develops or acquires new applications that enhance security. It is even possible that the payment card system could become obsolete with the development of alternative approaches to payments. As commentators have noted, the ubiquity of the Internet on our iPods, smart phones, automobiles, and televisions suggests that neat distinctions between payment transactions occurring in brick-and-mortar environments and online environments may be disappearing.60 Recent acquisitions of firms providing online payment solutions by payment card brands suggest that competition still exists, particularly in the online environment, despite the cooperative ventures for payment card security.61 By acquiring innovation from others in the marketplace, one member of the card brand oligopoly may indeed break out from the pack.

60. See Evans, supra note 31 (“The internet will become like the electric power grid—something that almost every device is plugged into. The corollary is that it will be meaningless to talk about internet-payment providers, such as PayPal, as if they were an interesting group of foreigners.”).
But for the time being, knowledge about security standards seems to be shared within the industry through the PCI SSC. The ongoing need to address changing technology presents a natural advantage for industry actors immersed in industry experiences as compared with government actors who are not. Constantly changing in complexity, knowledge asymmetry between the regulated industry and those who seek to regulate it presents significant challenges for government intervention. Consequently, the DSS, along with attendant processes and structures, are likely to remain intact for the foreseeable future, even if government chooses to intervene through some form of additional regulation.

The industry has also been sensitive to cost issues in implementing PCI DSS. While the development of standards and a compliance monitoring infrastructure has occurred on a cooperative basis, each card brand has made its own decisions about the implementation requirements for merchants who accept their card brand. For example, Visa divided merchant requirements into four tiers based on the number of transactions processed annually. Figure 5, below, summarizes the tiers and their requirements.62

As Figure 5 shows, only the largest firms—those with more than 6 million transactions—are subject to full annual compliance review by an independent QSA. Smaller firms are allowed to self-assess, with essentially no difference between firms in tiers 2 and 3, which have from twenty thousand up to six million transactions. The smallest firms, with fewer than twenty transactions, are subject to compliance validation requirements set by their acquiring bank.

MasterCard imposes similar compliance burdens and merchant tiers. Likewise, American Express imposes similar requirements on tier 1 and 2 merchants, but it imposes tier 1 responsibilities on those who process more than 2.5 million transactions and tier 2 responsibilities on those who process from 50,000 to 2.5 million transactions. Discover, in contrast, takes a “risk-based approach” for validation, the details of which are not disclosed.63 Card brands also reserve discretion to impose additional requirements, as both VISA and MasterCard may require a merchant who has experienced a breach to comply with tier 1 requirements.64

63. See id.
64. See id.
Figure 5: Compliance Validation (VISA, Inc.)

<table>
<thead>
<tr>
<th>Tier</th>
<th>Transactions</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| 1    | >6 million   | Annual report by QSA  
Quarterly network scan by ASV  
Attestation of Compliance |
| 2    | 1–6 million  | Annual SAQ  
Quarterly network scan by ASV  
Attestation of Compliance |
| 3    | 20,000–1 million | Annual SAQ  
Quarterly network scan by ASV  
Attestation of Compliance |
| 4    | < 20,000     | Annual SAQ (recommended)  
Quarterly network scan by ASV (if applicable)  
Compliance validation requirements set by acquirer |

Note:
QSA = Qualified Security Assessor  
ASV = Approved Scan Vendor  
SAQ = Self-Assessment Questionnaire

The industry thus chooses to direct the greatest compliance efforts toward securing the greatest number of transactions. In the process, it allows considerable latitude for small firms, for which compliance costs per transaction could be economically more burdensome. Basing the compliance burdens on transaction volume, which functions as a proxy for firm size, appears to take into account the significant costs associated with becoming PCI DSS compliant and maintaining that status. As reported in the PCI DSS Compliance Blog, top-level firms spent, on average, $2.7 million to become compliant in 2008, excluding the cost of PCI assessment services, which amounted to $237,000.65 In contrast, second level merchants spent an average of $1.1 million to become compliant and $135,000 for assessment. Level three merchants spent only $155,000 to become compliant. No data was collected from level four merchants.66 Larger firms presumably have a greater capacity to bear these substantial security costs than their

66. Id. (It is unclear how the levels reported in this study map to those of the varying card brands).
smaller counterparts. However, by choosing to include smaller merchants within the network, they have made a conscious decision—a business decision—to tolerate lower levels of security in the interest of obtaining higher market penetration and a more pervasive payment card network.\footnote{67}

Thus, to summarize, the private ordering mechanisms within the payment card industry are complex and have emerged to serve not only consumer interests, but also the interests of the commercial participants in the payment card network. These various relationships are summarized in Figure 6, below. Given the nature of private ordering solution—an extralegal mechanism with an elaborate set of processes, structures, and information—it is critical for the lawmakers to proceed with care. While a replacement of the entire mechanism \textit{in toto} would appear impractical, incursions that tinker with parts of the infrastructure and its attendant incentives could produce poor or incomplete solutions leading to dysfunctional or unintended consequences. The knowledge asymmetry between those inside the industry and those outside, combined with the need for requisite variety and the management of an elaborate infrastructure in light of changing technology, are powerful reasons for the law to promote and support the private ordering solution. As discussed below, one domain that the legal system should address and align involves disclosure requirements in relation to breaches of cardholder data security.

\textit{Figure 6. Foundations of Private Ordering within the PCI}

\footnote{67. The question may also be raised whether the political clout of this group of small businesses may have also spurred the policy of differential treatment in order to avoid regulation that may have imposed additional costs.}
IV. Legal Incursions on Private Ordering: An Assessment

As discussed above, economic incentives within the payment card network have provided the primary impetus for securing that network. However, assessments of PCI DSS suggest that significant non-compliance exists within the merchant community, often discovered after data breaches. A 2009 study by Verizon Business indicated that eighty-one percent of the victims of data security breaches were not PCI DSS compliant.68 A 2009 survey by the Ponemon Institute suggests that only twenty-two percent of firms are fully compliant across the enterprise, while twenty-eight percent are compliant for “most applications and databases” and twenty-five percent are compliant for “some applications and databases”; the remaining twenty-five percent are noncompliant.69

Data security breaches have continued to occur after the promulgation of PCI DSS, and those testifying in hearings before the House of Representatives Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology in early 2009 rehearsed a litany of breaches involving gaps in PCI DSS compliance.70 This is no surprise. Policymakers need to understand the impossibility of constructing a completely secure network and maintaining it in that state. However, technologists could construct a network that is sufficiently trustworthy to serve the needs of users.71 One can always take steps to enhance security, but such steps could impinge upon system functionality and usability, and are not cost free. The incidence of those costs, and their magnitude, deserves careful attention before intervening in the substance and procedure for security within a complex network. The discussion below evaluates significant examples of legal intervention and their effects on the private ordering regime.

69. PONEMON INST. LLC., 2009 PCI DSS COMPLIANCE SURVEY (2009), http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/PCI%20DSS%20Survey%20Key%20Findings%20FINAL4.pdf. It should be noted that these responses reflected approximately equal weighting from merchants in tiers one through four, thus reflecting a significant proportion of small firms in these compliance results. Given that high fixed costs make compliance economically difficult for small firms, these figures are likely to overstate the risk of insecurity. The percentage of total transactions that are secured would provide a more reliable indicator of overall security.
71. See VISA, supra note 54.
A. Disclosure Requirements

In the United States, the federal government has generally taken a sectoral approach to legislating protections for consumer privacy, thereby departing significantly from the comprehensive data protection regime found in the European Union. In this environment, the states have provided important leadership through legislation aimed at protecting the interests of consumers whose personal data may be disclosed. The imposition of disclosure requirements in connection with data security breaches has become a widely adopted practice under state law.

California started the trend toward disclosure requirements by enacting the first security breach notification law in 2002. Oddly, the data breach that is credited with precipitating California’s legislative response involved a government agency leaking state payroll information, where the agency delayed notification to the affected employees for several weeks. Government failure, rather than a failure in the private sector, served as the catalyst for legislation.

As of October 12, 2010, forty-six states plus the District of Columbia have enacted some form of data security breach notification law. Although there are differences in the particulars of these laws, they commonly require breaching firms (including government entities) to notify affected persons whenever their unencrypted personal information is believed to have been acquired by an unauthorized person.

---

72. See Morse & Raval, supra note 27, at 545 (citing Thomas J. Smedinghoff, It’s All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law, 16 MICH. ST. J. INT’L L. 1, 16 (2007)).


74. See id. at 1142–43.

75. Id. at 1143–44. As government lacks the private sector motivations for security that are rooted in reputational sanctions and other means of private ordering, a stronger argument may exist for public laws focusing on government behavior regarding data security than in the private sector. Id.


77. See CAL. CIV. CODE § 1798.82(e) (West 2008):

For purposes of this section, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account. (4) Medical information. (5) Health insurance information.

78. See id. § 1798.82(a) (West 2008):
Generally speaking, the state laws require direct notice unless the business demonstrates that the costs or scope of notification are particularly extensive, or if the business does not have sufficient contact information. In that case, the state law permits notice by e-mail (where possible) coupled with conspicuous posting of the notice on the company's website and notification of statewide media, in lieu of direct written communications.

The disclosure statute adopted in California and followed by other states effectively imposes a strict liability regime upon the breaching party. This approach imposes direct costs associated with disclosure upon the breaching firm, regardless of whether the firm had adequate security in place to deter an expected attack and regardless of whether the disclosure is likely to result in harm to the consumer. Some states have modified this regime to construct a different triggering mechanism, which exempts firms from disclosure if, after consultation with law enforcement, they reasonably believe that the disclosure "will not likely result in harm to the individuals whose personal information has been acquired and accessed."

Disclosure requirements thus alter the incentive structure for data security by imposing additional costs on firms that fail to protect their customers. The direct costs of disclosure are exacted outside the regime of private ordering. Of course, this assumes that firms comply

Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

79. See, e.g., id. § 1798.82(g) (allowing substitute notice where costs would exceed $250,000 or more than 500,000 persons would be involved).

80. See CAL. CIV. CODE § 1798.82(g)(3). The California statute allows firms to follow procedures in their own information security policies that are consistent with the timing requirements of the statute, thus recognizing that firms may undertake notification obligations as a result of their own privacy policies or contracts with customers. See id. § 1798.82(h).

81. See Winn, supra note 73, at 1147.

82. See id. (citing CONN. GEN. STAT. § 36a-701b(b) (2008)).

83. See Priscilla M. Regan, Federal Security Breach Notifications: Politics and Approaches, 24 BERKELEY TECH. L.J. 1103, 1123 (2009) ("Security breach notifications can be viewed as a mechanism for correcting that market imperfection [i.e., of underinvestment in security] by bringing to the organization's attention the cost of not adequately protecting data.").
with the legal obligation imposed upon them—a proposition that some critics doubt.84

But private ordering is important here, too, as disclosure also "hardens" the compliance regime within the payment card network. Disclosure also tends to ensure that the card network becomes aware of noncompliance, thus permitting the imposition of sanctions through their own regime. Moreover, disclosure allows reputational sanctions in the marketplace to function effectively. As noted in the 10-K reports of the payment card firms, disclosures may include adverse reputational effects, which go beyond the direct costs imposed on the unsecure merchant.85 Consumers may choose not to deal with unsecure merchants (at least using payment cards). A survey of 2,000 consumers published in 2008 indicates that sixty percent would blame the online merchant if the consumer became an identity theft victim after online shopping.86 This may not translate into lost sales in all cases, however, as other studies have indicated forty percent of consumers would consider terminating a retail customer relationship with a firm that experiences a data breach, but only nineteen percent actually do so.87

Moreover, to the extent that investors are sensitive to the costs that the unsecure firm incurs, management may experience additional incentives to be attentive to protecting customer information. Though customer information may not be perceived as an asset per se, the potential to impose significant costs if this information is not adequately protected should receive attention from management, much like the attention devoted to securing other firm assets.88

84. Winn, supra note 73, at 1148-49. Professor Winn argues that "because enforcement of... [security breach notification laws] depends almost entirely on self-regulation by owners of databases, then as a practical matter, organizations with good enough security policies to realize that they have a problem are exposed to much greater liability than organizations that are truly clueless." Id. at 1149. This may be true, but it would hardly be uncommon in a complex legal environment that depends on voluntary compliance. More sophisticated actors can generally be expected to be more aware of noncompliance, particularly when compliance obligations are known by many persons within the organization. Whistleblower provisions, similar to those designed to increase federal income tax compliance, may be particularly effective additions to the public law dimensions in this area. Cf. Edward A. Morse, Whistleblowers and Tax Enforcement: Using Inside Information to Close the "Tax Gap," 24 Akron Tax J. 1 (2009).

85. See Visa, supra note 45.

86. See First Data Comp. Intelligence, Consumer Online Shopping Fears (June 7, 2008), www.firstdata.com/en_us/insights/consumer-online-shopping-fears-study. However, the causal connection between identity theft and online shopping is often contestable. It can be difficult to trace identity theft to a particular disclosure, particularly when unsecure behavior is pervasive and it may include the consumer's own fault.

87. See Regan, supra note 83, at 1127.

Compliance costs for breaching firms are likely to be substantial, but estimates have varied considerably. For example, the General Accounting Office estimated notification costs averaging fifty-four dollars per record breached in 2007, while a private study by the Ponemon Institute in 2008 showed a cost of $197 per record breached.\textsuperscript{89} As these costs arise due to discrete, firm-specific events, affected firms would face difficulties in passing these on to consumers, at least in the short run, assuming competitive conditions in their product or service markets.

In theory, disclosure laws encourage notice to consumers of increased probability of potential harm, which the firm would otherwise prefer not to disclose. This may provide consumers with an opportunity to take steps to protect themselves, such as monitoring credit reports or placing a hold or freeze on the opening of new accounts.\textsuperscript{90} However, the potential harm to a consumer is uncertain and highly speculative, making it difficult to determine whether responsive action is appropriate.\textsuperscript{91} As some commentators have pointed out, consumers who terminate their relationship with a breaching firm and open a new relationship with another firm may actually increase their risk exposure by further spreading their personal information in the marketplace.\textsuperscript{92} Only a small percentage of consumers who were offered credit protection and monitoring tools after one major breach took advantage of those benefits, and many consumers simply ignore breach notification letters.\textsuperscript{93} This may not be an irrational choice, as it is far from clear that experts can trace data security breaches directly to a criminal incident. Moreover, some consumers already take these

\textsuperscript{89} See Winn, supra note 73, at 1149.
\textsuperscript{90} See Morse & Raval, supra note 27, at 547.
\textsuperscript{91} See Romanosky & Acquisti, supra note 44, at 1094. Recent case law has generally rejected consumer claims based on the enhanced potential for identity theft as either failing to present an "injury-in-fact" for purposes of legal standing to sue, or alternatively if deemed sufficient for standing (which requires only a minimal standard), on the basis that there is an insufficient injury for purposes of the underlying state law claim. See, e.g., Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009) (dismissing class action for data security breach as failing to present an injury-in-fact for purposes of standing, and alternatively for failing to state a claim under Missouri law).
\textsuperscript{92} Romanosky & Acquisti, supra note 44, at 1095.
\textsuperscript{93} See id. at 1097.
steps to protect themselves from these risks by purchasing security services from third parties, and personal disclosure to them presumably adds little to the protection they have already acquired through contract.

Just as disclosure may be helpful to trigger enforcement efforts within the card network, including fines or other sanctions, it may also prove useful to others in the marketplace, including issuing banks that may choose to take additional security steps. These additional security steps might include cancelling and reissuing cards or modifying algorithms to detect the "red flags" of fraud. Moreover, government agencies (such as the FTC, as discussed below) may also use disclosure as the basis for additional intervention.94

While disclosure may be an important feature to reinforce both reputational sanctions in the marketplace and internal sanctions in the payment card networks, it may be possible to achieve these important benefits while also lowering the costs of particularized notice to consumers. To the extent that behavioral economic theory suggests that consumers may not behave rationally with regard to the information concerning a security breach,95 limiting disclosure to public forums—such as the company website—may be sufficient to allow network and reputational sanctions to function effectively. By disclosing the context of the breach, the market can presumably ascertain whether the firm behaves responsibly with regard to security and punish it appropriately. Such an approach might enhance consumer welfare more than one that imposes a "tax" or "penalty" on responsible and irresponsible firms through personalized disclosures, which may not benefit consumers.

Such an approach would not necessarily displace private ordering, but would strengthen both the internal functions (i.e., within the card network) and the market functions (i.e., reputational sanctions, particularly those that are reinforced through public securities markets) that help to incentivize behavior. To the extent individual notice is important to consumers, they could contract with private firms (for example, credit monitoring services), thus providing a private solution that is less costly and more efficient. Data security breach costs may also become part of another private ordering regime—namely, insur-

94. See id.
95. See id. at 1096 ("[R]esearch in behavioral economics and behavioral decision making provides ample evidence that consumers are unable to conceive of all possible outcomes and risks of data disclosures.").
For insured firms, an additional private actor—the insurer—will also have an interest in monitoring security practices, thereby providing additional support for security enhancement.

The state-level disclosure regime outlined above has not yet been displaced by a federal law that requires disclosure for security breaches, though proposed legislation has been working its way through Congress. Variation in requirements among the states potentially creates significant problems for firms engaged in multijurisdictional business operations, which might be solved by uniform requirements within a federal statute. Moreover, states have limited geographic reach due to jurisdictional concerns for commerce. As discussed below, a federal solution may resolve these problems. However, federal preemption of state laws presupposes that a correct solution has been designed—a contestable proposition based on the analysis provided above.

B. Reallocating Externalized Costs

Parties dissatisfied with outcomes under the private ordering regime have sought to reallocate their losses through litigation. The payment card network does not offer direct contractual links between all of the parties affected by a breach, thus providing an apparent limit on the effectiveness of private ordering through contract. For example, a bank that issues a payment card to a consumer may incur costs associated with cancelling and reissuing a card because of disclosure by a merchant. Although a payment card network may punish the merchant for being unsecure (probably indirectly, through an agreement with the merchant's acquiring bank which may impose a fine or other sanctions), a payment card network has not required unsecure merchants to indemnify the issuing banks for these costs.

Likewise, a consumer may experience ancillary costs outside the network, such as lost time and frustration from contesting fraudulent charges against his accounts. The consumer may not have any contractual basis for recovering against the merchant who was responsible for releasing cardholder data. Moreover, the consumer would face a difficult task in proving causation on account of the merchant's un-
secure behavior, as a lack of security does not necessarily produce fraud.\textsuperscript{100}

Litigation has proven to be a somewhat ineffective vehicle for developing an alternative legal path to recovering these losses, as courts have rejected many such claims. However, legislation giving recourse to issuing banks has emerged in three states: Minnesota, Nevada, and Washington, albeit with very different approaches to the matter of assessing liability and the expected levels of compliance to shield a merchant from liability. Each of these legal paths is discussed below.

1. Litigation

In the litigation surrounding TJX’s payment card data security breaches, issuing banks sued TJX for the costs externalized to them, which included cancelling compromised cards and reissuing new ones; also, state attorneys general sued TJX under consumer protection laws. The company has settled all claims.\textsuperscript{101} Such settlements reflect private ordering that is guided by public laws and public courts. However, the particular claims invoked in these cases suggest considerable uncertainty as to the legal basis for recovery if these cases had continued to judgment.\textsuperscript{102}

As courts have pointed out, contract is an inadequate basis for security obligations in this context, as there is no privity of contract between a merchant, such as TJX, and a bank issuing a payment card to a retail customer that is used to pay the merchant.\textsuperscript{103} Tort also provides an inadequate basis for a claim because the economic loss doctrine commonly bars recoveries where damages are purely economic and do not involve property damage or other physical injury.\textsuperscript{104}

Consumer plaintiffs have had difficulty establishing the legal standing to bring suit, given that the existence of a breach does not necessa-

\begin{itemize}
  \item \textsuperscript{100} See Romanosky \& Acquisti, supra note 44, at 1094 ("[F]or a plaintiff, it is difficult to prove that the harm originated from a particular instance of data breach: the victim may not be even aware that his data was in the possession of a certain firm, may not know that his data has been breached, and may not be able to connect the harm born to the actual breach—since his data may have been available at the same time to many other merchants or third parties.").
  \item \textsuperscript{101} See Morse \& Raval, supra note 27, at 547-49; Morse \& Raval, supra note 88, at 32–35 (recounting in some detail the various cases arising under this breach).
  \item \textsuperscript{102} See Morse \& Raval, supra note 88, at 35 ("[C]oming out of this litigation, we are left with considerable uncertainty from the judicial sector as to what standard of behavior is required with regard to data security and the basis for a successful claim.").
  \item \textsuperscript{103} See Morse \& Raval, supra note 27, at 548–49 (indicating that the merchant’s bank, which provides processing services for customer payments, also lacks privity, as the court in TXJ recognized).
  \item \textsuperscript{104} See id.
\end{itemize}
rily translate into actual damages.\textsuperscript{105} Moreover, the kind of damages that should be cognizable in such actions remains controversial. In recent litigation, a federal district court has submitted a certified question to the Supreme Judicial Court of Maine to ascertain whether time and effort alone sufficiently constitute an injury, and if so, whether such economic harms could serve as the basis for recovery under applicable state law.\textsuperscript{106}

Although courts have the capacity to fashion appropriate remedies for legal wrongs, they seem poorly suited as forums for complex rulemaking in a manner that could seriously displace private ordering. Reallocating losses after a breach has occurred can incentivize prophylactic behavior by merchants to enhance security for consumers and others affected by payment card data breaches. However, the facts presented by the litigants before the court limit the context for rulemaking. This engenders a piecemeal development process, which necessarily leaves the precise behavioral standard to development in future cases.

2. Legislation

Legislative solutions to this problem have also emerged at the state level. Three different approaches have emerged, and each provides a useful learning tool with regard to the ultimate impact upon the data security environment.

\textit{Minnesota.} Minnesota was the first state to adopt legislation that effectively protects issuing banks from costs incurred to protect cardholders, including cancellation, reissuance, and notification. It also protects banks from the costs of unauthorized transactions.\textsuperscript{107} This weak standard for liability only requires a finding of liability when breach occurs if the merchant retains customer information more than 48 hours after the transaction authorization.\textsuperscript{108} This falls far short of

\textsuperscript{105} See id.; see also Romanosky & Acquisti, \textit{supra} note 44, at 1094 (noting causation and proof issues); see also \textit{Identity Theft Survey Report, supra} note 48, at 32 (noting the majority of victims (fifty-six percent) did not know how their information was stolen).

\textsuperscript{106} See \textit{In re Hannaford Bros. Co. Customer Data Sec. Breach}, 671 F. Supp. 2d 198 (D. Me. 2009), \textit{cert. granted}, 4 A.3d 492 (Me. 2010). The Maine Supreme Judicial Court concluded that time and effort alone do not constitute a cognizable injury recoverable in an implied contract claim. \textit{See In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.}, 4 A.3d 492, 497–98 (Me. 2010). However, the First Circuit has ruled that an implied contract claim may go forward based on damages from costs incurred for mitigation of risks, such as credit monitoring or card replacement fees. \textit{See Anderson v. Hannaford Bros. Co.}, 659 F.3d 151, 165-66 (1st Cir. 2011).


\textsuperscript{108} See id. § 325E.64(2).
PCI DSS requirements. However, by threatening significant liability for a subset of behavior that may be deemed highly improper according to emerging customary data security standards, this approach sends a significant signal to merchants as to their need for appropriate security. Perhaps for this reason, there are no exemptions for small merchants built into this legislation, thereby subjecting all actors to the potential threat of litigation.

Nevada. Nevada has enacted legislation that became effective January 1, 2010, to require either compliance with PCI DSS or encryption in connection with the transmission of any payment card data. Section 1 provides:

If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization.

This legislation thus expressly adopts and brings in PCI DSS compliance, including monitoring functions, as a matter of state law. Rather than freezing the standards in time, it allows the industry to determine what changes are required and the timetable for compliance.

Alternatively, this law provides that those who do not comply with PCI DSS may not electronically transmit personal information or move any storage device containing personal information “beyond the logical or physical controls of the data collector” unless encryption is used “to ensure the security of the information.” This law fails to prescribe the type of encryption required, leaving such matters undefined. If a weak encryption standard is used, it is highly doubtful that this would “ensure the security of the information” against a clever attacker. Encryption involves a complex set of choices, including the selection of end-points for data on the move, choice of algorithm, key length, use of certificates in public key cryptography, and key manage-

111. See id.; see also id. § 603A.030 (defining a “data collector” to include “any governmental agency, institution of higher education, corporation, financial institution, or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information”).
112. See id. § 603.215(2)(a)–(b).
ment approaches,\textsuperscript{113} which potentially illustrate the problem of knowledge asymmetry between legislators and the industry experts. Although undefined encryption standards avoid the problem of encapsulating past technology into the legal standard, this approach could also fail to achieve the protective goal intended for the statute.

Significantly, this legislation does not expressly provide a private cause of action or impose a penalty for noncompliance. Nevada law does empower the “data collector” to bring a civil action against a person who unlawfully obtained or benefited from personal information maintained by the data collector, thus permitting recovery against unauthorized users.\textsuperscript{114} Damages may include costs incurred in notifying its customers.\textsuperscript{115} However, injunctive relief against the data collector is available only to the extent the attorney general or district attorney has reason to believe the data protection requirements are being violated.\textsuperscript{116}

When, as here, the legislature has spoken directly to the matter of compliance and data security, query whether a court will interpret this legislative behavior as expressing an intention to preclude the development of further private remedies. To the extent any other private causes of action may be developed, Nevada law asserts that compliance with either the PCI DSS or encryption requirements provides a shield against liability. However, in order to obtain this liability shield, the data collector must show: “(a) The data collector is in compliance with this section; and (b) [t]he breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees, or agents.”\textsuperscript{117}

By stating these requirements conjunctively, the liability shield may be modest indeed for those seeking protection by PCI DSS compliance. Compliance with PCI DSS may be certified at a given point in time, but any change in circumstances following certification could make a system fail to be in compliance, although not clearly recognized or assessed as such. In that case, a breach occurring due to some form of human error, even though not rising to the level of gross negligence or intentional misconduct, could cause the data collector to lose its shield. Moreover, this could occur without the knowledge of

\textsuperscript{113} See generally Vasant Raval & Ashok Fichadia, Risks, Controls, & Security 120–68 (Wiley 2007).

\textsuperscript{114} See Nev. Rev. Stat. § 603A.900 (2006). Of course, this presupposes that the hacker is identified and subject to jurisdiction in a court that will apply this law.

\textsuperscript{115} See id. § 603A.910.

\textsuperscript{116} See id. § 603A.920.

\textsuperscript{117} Id. 603A.215(3).
the data collector, leaving extant the threat of liability regardless of
the degree of compliance undertaken.

This legislation makes no apparent distinctions in protective efforts
based on the size or transaction volume of the data collector. Given
the economics of PCI DSS compliance, this approach imposes poten-
tially significant burdens upon small merchants seeking protection
from litigation risks. Such merchants may only take comfort in know-
ing that the economics of litigation may also favor them, to the extent
that the prospects for damage recovery may be limited and thus make
litigation unattractive to a potential plaintiff.

Washington. The Washington legislature enacted a new law on
March 22, 2010, that became effective on July 1, 2010.118 This bill
states the legislature's intent "to encourage financial institutions to re-
issue credit and debit cards to consumers when appropriate, and to
permit financial institutions to recoup data breach costs associated
with the reissuance [of compromised cards] from large businesses and
card processors who are negligent in maintaining or transmitting card
data."119 In contrast to the Nevada legislation, the Washington law
expressly limits its impact to large businesses, defined to include an
entity (including government) that "processes more than six million
credit card and debit card transactions annually, and who provides,
offers or sells goods or services to persons who are residents of Wash-
ington."120 Those who process card transactions are also included, as
well as vendors who sell software for these purposes.121

The bill provides a private cause of action for damages in favor of
financial institutions affected by a breach. In particular, the bill
provides:

If a processor or business fails to take reasonable care to guard
against unauthorized access to account information that is in the
possession or under the control of the business or processor, and the
failure is found to be the proximate cause of a breach, the processor
or business is liable to a financial institution for reimbursement of
reasonable actual costs related to the reissuance of credit cards and
debit cards that are incurred by the financial institution to mitigate
potential current or future damages to its credit card and debit card
holders that reside in the state of Washington as a consequence of
the breach, even if the financial institution has not suffered a physi-
cal injury in connection with the breach.122

118. 2010 Wash. Sess. Laws 1055, § 3. The law applies prospectively to breaches on or after
the effective date. Id. § 4.
119. Id. § 1.
120. Id. § 2(1)(c).
121. See id. §§ 2(1)(h) (defining "processor"), (j) (defining "vendor").
122. Id. § 2(3)(a).
The bill also provides for the recovery of attorney’s fees, thus reversing the typical “American Rule” applicable to attorney’s fees and turning this kind of litigation into a “loser pays” scenario, thus further raising the stakes for the parties.\textsuperscript{123}

Vendors also face liability based on damages proximately caused by the vendor’s negligence, but only if “the claim is not limited or foreclosed by another provision of law or by a contract to which the financial institution is a party.”\textsuperscript{124} Thus, a software provider that fails to prevent an unanticipated security breach may also face liability, despite the fact that its contract with a merchant customer contains a warranty provision that limits its damages. In this sense, this vendor liability provision may truly raise the stakes for software developers, creating a new risk that has thus far been remote. When more than one party shares responsibility for the breach, the trier of fact must allocate damages among them.\textsuperscript{125}

Fortunately for affected entities, the statute has a safe harbor provision to protect against liability. The safe harbor provides in part:

Processors, businesses, and vendors are not liable under this section if (a) the account information was encrypted at the time of the breach, or (b) the processor, business, or vendor was certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach.

Similar to the Nevada legislation, the statute allows for either compliance or encryption. However, for this purpose, “encryption” is defined to mean “enciphered or encoded using standards reasonable for the breached business or processor taking into account the business or processor’s size and the number of transactions processed annually.”\textsuperscript{126} Thus, Washington attempts to provide a context for defining encryption, which Nevada fails to do.

As for compliance, this bill treats validation by an annual security assessment within the past year as conclusive protection against liability. The bill provides in part:

A processor, business, or vendor will be considered compliant, if its payment card industry data security compliance was validated by an annual security assessment, and if this assessment took place no more than one year prior to the time of the breach. For the pur-

\textsuperscript{123} See id.
\textsuperscript{124} 2010 Wash. Sess. Laws 1053, § 2(3)(b).
\textsuperscript{125} See id. §§ 2(5) (allowing defenses of contract or of contributory or comparative negligence), (6) (charging trier of fact with duty to determine percentage of fault attributable to every entity).
\textsuperscript{126} Id. § 2(1)(f).
poses of this subsection (2), a processor, business, or vendor's security assessment of compliance is nonrevocable. The nonrevocability of a processor, business, or vendor's security assessment of compliance is only for the purpose of determining a processor, business, or vendor's liability under this subsection (2).\footnote{Id. § 2(2).}

Washington's approach solves the problem of defining compliance, which the Nevada law failed to do. As long as compliance certification has been achieved (a process which also involves private ordering, as there is no government-based accreditation standard for assessing compliance), the entity may not be held liable under this section. This liability shield apparently applies even if the entity may be shown to be grossly negligent in handling data or in implementing PCI DSS at the time the breach occurred.

The Washington legislation may channel behavior toward PCI DSS compliance through an annual assessment process (thereby providing an ancillary benefit to service providers in the form of a built-in demand apart from private ordering within the card industry for third-party compliance certification).\footnote{This form of embedding PCI DSS was also adopted by the State of Texas. On May 11, 2007, the Texas House of Representatives unanimously passed HB 3222, which mandates that businesses that accept payment cards comply with all PCI DSS requirements effective January 1, 2009). See H.B. 3222, 80th Leg., Reg. Sess. (Tex. 2007).} However, whether the bill achieves its goal of providing marginal benefits to consumers by incentivizing payment card issuers to reissue compromised cards seems dubious. Whether card issuers need additional incentives has not been proven, given that they must deal with claims for unauthorized charges from cardholders with compromised security. The avoidance of those costs, alone, would likely generate sufficient incentives for reissuance in many cases.\footnote{In fact, the potential recovery of costs and attorney's fees may induce a moral hazard in the event that circumstances might indicate that disclosure of account information presents a low risk of compromise for consumers. In this sense, the recovery may be inefficient.}

A liability safe harbor based on certification within the past year does not seem to add much to the security of the payment card system beyond that already required by private ordering. In fact, larger firms must receive validation of compliance more often than annually under current private ordering rules.\footnote{Although it may induce some smaller firms to move from a regime of self-validation to independent validation, this may have the unintended consequence of significantly raising costs for these smaller firms, which may be unable to afford the substantial fixed costs associated with annual certification. Thus, an unintended consequence of intervention may be to enhance the ad-}
vantages of larger firms over smaller ones. These considerations apparently influenced Governor Schwarzenegger of California, who vetoed a similar bill favoring issuing banks on the basis that it would unfairly harm small businesses and that "the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers."131

These three state laws provide divergent approaches to legislation, which may provide some insights regarding their impact on the private ordering regime. To varying degrees, they seek to induce behaviors that will enhance security as a byproduct of granting a post hoc benefit to issuing banks. Instead of creating a direct benefit to consumers, the putative benefits are designed to flow through to them indirectly: first, by incentivizing merchants to invest in security by forcing them to internalize additional costs that arise from a security breach; second, by incentivizing issuing banks to engage in risk-avoidance behaviors that are likely to protect consumers; and third, by preventing consumers with account relationships from the consequences of additional costs incurred by issuing banks.

The first and last reasons noted above are closely related. By reallocating costs from the unsecure merchant to the issuing bank, consumers with relationships to the issuing bank will likely experience a reduction in their total costs. Conversely, those consumers may end up paying more for goods at these merchants, which must ultimately take into account security costs. But apart from the cost reallocation, it remains unclear whether consumer welfare will be enhanced, particularly if there are significant transaction costs associated with litigation. As for the second reason, as previously stated, issuing banks hardly need additional incentives to protect the security interests of their cardholders. Although issuing banks are unlikely to experience the direct costs of fraudulent charges (which are charged back to the merchant in many cases),132 the indirect costs associated with customer relations, (e.g., addressing fraud claims, resolving disputes, and the like) are real costs that issuing banks must address, and therefore are incentivized to avoid. Moreover, issuing banks have also experienced some nudging toward security monitoring behavior from the federal government, which has imposed a so-called "red flags rule" through the FTC and through bank regulatory agencies to require fi-


132. In some cases, issuing banks may indeed bear some of these fraud losses. For example, issuing banks bear fraud losses associated with debit cards where PIN requirements are satisfied. See MacCathy, supra note 131, at ¶ 33.
nancial institutions and other creditors to implement monitoring protocols designed to inform customers when fraud may be present.\textsuperscript{133}

These state laws reflect another problem, which is endemic to state-based legislation: the scope of protection is necessarily limited due to geographical boundaries. For example, in the Washington legislation, a business need not be physically present in Washington for this law to apply; the law includes one “who provides, offers, or sells goods or services to persons who are residents of Washington.”\textsuperscript{134} This rule potentially reaches beyond the state’s borders, but as a practical matter a successful plaintiff must overcome jurisdictional barriers in seeking to litigate the rights granted by these statutes.

C. Federal Intervention: The FTC, the Fed, the CFPB, and Beyond?

The discussion above has illustrated several specific examples of state-law intervention upon the private ordering regime. The federal government has intervened extensively in the credit aspects of the payment card industry, which has included massive legislative and regulatory reform.\textsuperscript{135} Behavioral economics has played a large part in this regulation, where private ordering has clearly been disrupted through prescriptions that are designed to protect consumers from practices the government deems unfair.\textsuperscript{136}

However, in matters of security, federal intervention has been limited in the area of legislation, but greater in the matter of discretionary intervention from regulatory agencies. As discussed below, the legislative incursion has proved disastrous, while discretionary intervention has injected additional uncertainty into the marketplace. Neither of these approaches has clearly delivered improvements on the private ordering regime.

1. Legislating Security: FACTA

The Fair and Accurate Credit Transactions Act of 2003 (FACTA)\textsuperscript{137} includes provisions that target a very narrow problem—credit card


numbers and expiration dates displayed on printed receipts. Since receipts could easily fall into the wrong hands, FACTA requires merchants to truncate credit and debit card numbers, limiting that display to no more than the last five digits, and to block out expiration dates on printed receipts.

However, this statutory regime applies only to “receipts that are electronically printed.” Transactions that generate receipts by handwriting or by taking an imprint or making a copy of the card are expressly exempted. FACTA’s restriction clearly fits the retail merchant in a brick-and-mortar operation that electronically scans a payment card and gives an electronic receipt to a customer. It does not fit smaller merchants using carbon-based forms to take imprints of the customer’s card. Although technology and the desire to limit processing costs (both the product of private ordering within the payment network) would gradually eliminate those carbon paper forms, it appears that Congress was sufficiently concerned about the potential costs associated with changing to new systems that required all merchants to adopt new technology, despite the risks presented by paper forms displaying full card information.

Viewed from an economic perspective, this restrictive approach toward reducing security risks may be justified when the expected consumer harm (and merchant losses) from reduced access to payment options may outweigh the limited marginal risk from the low-volume and high-cost form of identity theft based on carbon forms. However, in terms of addressing the real costs of crime, paper receipts would likely present a higher-cost alternative for a prospective fraudster than unencrypted electronic data, which is not covered by FACTA. In this sense, FACTA is highly underinclusive, particularly considering recent Seventh Circuit interpretation of the Act as not applying to electronic receipts.
FACTA is also overinclusive to the extent that the statute potentially subjects merchants to sanctions for behavior that poses no meaningful risk to consumers. Consider, for example, *Bateman v. American Multi-Cinema, Inc.* in which the AMC movie theater chain allegedly printed the first four and the last four card numbers of their customers on some 290,000 printed receipts. The middle eight card digits were still blocked, however, leaving a potential fraudster with the prospect of choosing from among 100 million different combinations in order to find the functional card number. A FACTA violation could also occur if the merchant disclosed only the expiration date on a payment card, without disclosing any other card numbers. This likewise presents no appreciable risk to consumers in the absence of other information.

Other federal laws or regulations dealing with consumer financial privacy, such as Gramm-Leach-Bliley, generally rely on regulatory agencies for enforcement. This ensures that agency discretion can be brought to bear in determining the appropriate result for a putative violation. However, FACTA permits enforcement through litigation by consumers affected by unlawful disclosure. Whereas actual damages are likely to be limited or even nonexistent—a phenomenon that is recognized in other litigation based on data security breaches—FACTA provides an option to pursue statutory damages ranging from $100 to $1,000 for every willful violation, along with the recovery of attorney’s fees. Combining this provision with class action litigation can thereby transform a disclosure causing little or no actual consumer harm into a significant liability event for a noncompliant merchant. For example, in *Bateman,* the Ninth Circuit allowed

144. 623 F.3d 708 (9th Cir. 2010).
145. See § 1681c(g)(1) (restricting the display of “more than the last 5 digits of the card number or the expiration date”) (emphasis added). See, e.g., *Shlahtichman,* 615 F.3d at 796 (alleging FACTA violation based solely on disclosure of expiration date).
146. See, e.g., § 6805 (delegating enforcement authority to federal functional regulations, state insurance authorities, and the Federal Trade Commission).
147. For a recent case taking up the issue of whether an increased risk of identity theft could be considered as a basis for Article III standing, see *Krotten v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).
148. See 15 U.S.C. §1681n. FACTA shares this statutory damage provision with the Fair Credit Reporting Act, which has likewise been interpreted by the Seventh Circuit as eligible for class certification despite the potential for damages that are significantly greater than actual harm. See *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 951 (7th Cir. 2006).
149. 623 F.3d 708 (9th Cir. 2010).
class certification for a FACTA violation despite the fact that AMC’s potential liability was “enormous and out of proportion to any harm suffered by the class.”150

Congress has recognized that the FACTA enforcement regime had generated significant class action lawsuits against merchants. In 2008, it amended FACTA to address litigation against merchants who had erroneously disclosed only the card expiration date.151 Merchants had apparently misread the disjunctive construction of the statute and printed receipts with truncated card numbers along with expiration dates, triggering hundreds of lawsuits to collect statutory damages for a willful violation. As Congress had explained in connection with this amendment, “[T]he purpose of this Act is to ensure that consumers suffering from any actual harm to their credit or identity are protected while simultaneously limiting the abusive lawsuits that do not protect consumers but only result in increased cost to business and potentially increased prices to consumers.”152

However, the safe harbor protection enacted was narrowly crafted to exempt expiration date disclosures between December 4, 2004 and June 3, 2008 from the category of willful violations eligible for statutory damages.153 Although aware of class action litigation involving FACTA (and thus able to surmise the potential for large statutory damage awards), Congress did not restrict the class action remedy or impose a cap on recoveries, which it had done in other contexts involving statutory damages.154

*Bateman* illustrates that FACTA may provide windfalls for “bounty hunters” motivated by the profit potential from statutory damage awards coupled with attorney fees, but those awards come at a significant cost to consumers. Although the liability threat from statutory damages may indeed induce greater merchant vigilance, the disproportionate nature of that liability in relation to consumer harm will likely trigger overinvestment by merchants in monitoring and compliance (in relation to the real risks of causing actual damages), buying essentially no marginal protection for consumers in return.

In cases involving minor infractions of FACTA, litigation costs effectively purchase no benefits from enhanced security. In enacting the

---

150. *Id.* at 710.
152. *Id.* § 2(b).
154. See *Bateman*, 623 F.3d at 720–21 (noting damage caps added to the Truth in Lending Act).
Clarification Act in 2008, Congress made a rare admission that FACTA effectively harmed consumers through raising litigation costs. Nevertheless, Congress chose to leave the statutory liability regime in place, even when violations did not present risks of consumer harm. This is hardly an improvement over private ordering, and in fact shows quite the opposite effect. Payment card data security standards emerging after 2003, as discussed below, would ultimately provide greater protection, and without the significant external costs associated with the private bounty system, which persist to this day.

2. Discretionary Protection by the Federal Trade Commission

The FTC, operating under its authority to address unfair trade practices, has also provided an important federal presence in driving data security practices. We have elsewhere chronicled the efforts of the FTC to bring actions against large firms that have failed to maintain the security of their customers’ data, including actions against Choicepoint, TJMaxx, and Heartland Payment Systems. This general authority may serve a useful purpose in providing an additional threat against behavior that the agency may characterize as “unfair” and thus within the scope of its powers, including the power to impose monetary penalties and to require remedial behavior. Moreover, the discretionary approach for enforcement by an agency that has limited resources may present a greater likelihood that those resources will not be addressed on merely technical violations that present no meaningful threat to consumer well-being.

The discretionary nature of current FTC powers presents its own basis for concern. As long as the parameters of what is “unfair” are undefined by regulation, a potential exists for this power to be abused. Uncertainty may present some impetus for additional security innovation within the private sector, which is designed to keep ahead of the need for government interference.

Threats of greater regulatory authority to be exercised by the FTC have been presented in recent legislation. Late in 2009, the House passed H.R. 2221, the Data Accountability and Trust Act, which addressed several aspects of the data security breach problem. It included a federal notification rule for data security breaches, thus preempting the state laws on this subject. It also delegated author-

156. See Morse & Raval, supra note 27; Morse & Raval, supra note 88.
158. H.R. 2221 § 3.
ity to the FTC to promulgate regulations “to require each person engaged in interstate commerce that owns or possesses data containing personal information, or contracts to have any third party entity maintain such data for such person, to establish and implement policies and procedures regarding information security practices . . . .”

These regulations would preempt state information security laws, thereby ensuring a single federal source for compliance.

Although businesses may prefer a single federal source for law, thereby avoiding the complexity of a patchwork of state rules, the prospects of expanding agency power leave open the problem of prescribing content to new regulations. For example, with regard to payment systems, would the FTC choose to “in-source” the PCI DSS infrastructure, including compliance mechanisms, and perhaps make them more robust? Would the compliance requirements continue to be prescribed in a manner that respects the differential ability between small and large firms to bear the significant costs of acquiring and maintaining a PCI DSS infrastructure? There are many unanswered questions with this legislation’s attempt to delegate regulatory power. The problems of data security breaches surely go beyond the payment card industry, and many nuanced questions concerning the appropriate standards for different kinds of data remain, which the payment card industry has not addressed.

It should be noted that the legislative approach in HR 2221 continued present law in failing to provide a private cause of action for data security breaches. Thus, this bill would not repeat the inefficient bounty system that was exposed in FACTA. However, it would grant enforcement powers to the FTC and state attorneys general, including the imposition of civil penalties and fines, not to exceed a total of $5 million.

Although this bill expired when the 111th Congress adjourned in 2010, it is possible that others like it will emerge in the 112th Congress. However, as discussed below, there may be new sheriffs in town, which could displace the FTC’s role in this area.

159. Id. § 2(a)(1).
160. See id. § 6.
161. See FACTA supra note 137, at 18.
162. See H.R. 2221 § 4.
3. Other Competing Federal Regulators

It appears that the primacy of the FTC as the locus of federal authority for data security matters affecting payment cards may be challenged by other federal agencies, including the Federal Reserve and other functional federal regulators in charge of banks. The Dodd-Frank Wall Street Reform and Consumer Protection Act\textsuperscript{164} creates a new agency, the Bureau of Consumer Financial Protection, established within the Federal Reserve System, which “shall regulate the offering and provision of consumer financial products or services under the Federal consumer financial laws.”\textsuperscript{165} The purpose of the Bureau is stated as follows: “The Bureau shall seek to implement and, where applicable, enforce Federal consumer financial law consistently for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumers financial products and services are fair, transparent, and competitive.”\textsuperscript{166} Although at first glance one might conclude that the Bureau’s focus may not be directed to data security practices, it should be noted that the objectives of the bureau include ensuring that “consumers are protected from unfair, deceptive, or abusive acts and practices. . . .”\textsuperscript{167} Of course, as the FTC has demonstrated, poor data security practices may indeed be “unfair practices” for purposes of implementing its consumer protection powers.\textsuperscript{168}

Provisions in Dodd-Frank appear to contemplate that the FTC and the Bureau will negotiate their enforcement roles in areas where their authority may overlap.\textsuperscript{169} Moreover, the Bureau has received express grants of enforcement authority over any rule prescribed by the FTC “with respect to an unfair or deceptive act or practice” when it affects consumer protection matters covered by the Bureau.\textsuperscript{170} Although the Bureau has not yet exercised its enforcement or rulemaking pow-

\textsuperscript{166} Id. § 1021(a) (codified at 12 U.S.C. § 5511).
\textsuperscript{167} Id. § 1021(b)(2).
\textsuperscript{168} See \textit{supra} note 156.
\textsuperscript{170} See \textit{id.} § 1061(b)(5), 124 Stat. 2037.
ers,\textsuperscript{171} it remains to be seen whether the Bureau will take on the issue of data security standards for payment cards.

Elsewhere in the Federal Reserve, the issue of payment card data security standards is currently on the front burner in the form of a regulation project. The so-called “Durbin Amendment,” Section 1075 of Dodd-Frank, grants regulatory authority to the Federal Reserve to address “reasonable fees and rules for payment card transactions.”\textsuperscript{172} This general grant of authority may ultimately involve regulations dealing with data security requirements, to the extent that fraud prevention measures may have an impact on the cost structures associated with payment card fees charged within the network. Proposed regulations issued on December 28, 2010,\textsuperscript{173} included a request for comments on proposals to address fraud prevention measures:

The Board’s proposal requests comment on two general approaches to the fraud-prevention adjustment framework and asks several questions related to the two alternatives. One approach focuses on implementation of major innovations that would likely result in substantial reductions in total, industry-wide fraud losses. The second approach focuses on reasonably necessary steps for an issuer to maintain an effective fraud-prevention program, but would not prescribe specific technologies that must be employed as part of the program. At this time, the Board is not proposing a specific adjustment to the amount of an interchange fee for an issuer’s fraud-prevention costs. After considering the comments received, the Board expects to develop a specific proposal on the fraud adjustment for public comment.\textsuperscript{174}

The regulatory path that will ultimately be chosen here is unclear. However, the private ordering regime is under scrutiny, and more than one federal agency may ultimately become involved in deciding how the payment card industry should deal with the matter of security. The target of these regulations will nominally be large issuing banks, as the Durbin Amendment purports to exempt small issuers, defined as those with assets of less than $10 billion, from the impact of required rulemaking.\textsuperscript{175} However, the practical import of that limita-

\textsuperscript{171} The CFPB’s website discusses its current activities, which appear to be mostly educational. See Consumer Fin. Protection Bureau, www.consumerfinance.gov (last visited Jan. 11, 2012). The website explains that “[m]any of the prices of the Dodd-Frank Act relating to the CFPB will go into effect on July 21, 2011.” Id.


\textsuperscript{174} Id. at 81,722.

tion throughout the network also remains to be seen. Payment networks function efficiently and effectively across a broad range of participants, and as a practical matter, regulatory choices that emerge in this context will likely affect all participants, perhaps through intervention by the card networks. The bottom line question is this: Is the mosaic of regulation at state and federal levels hindering rather than helping institute a sound market model? Should the policy makers be seeking ways to empower the private ordering solution?

V. SUMMARY OF POLICY AND RESEARCH ISSUES; CONCLUDING OBSERVATIONS

In a rather comprehensive analysis and discussion of the private ordering realm of the payment card industry, we have identified three distinct facets of the problem space: (1) Ubiquity of the infrastructure, its global reach and technology dependence; (2) the infrastructure of PCI DSS and its strengths and limitations; and (3) the incursions of regulations and laws, including disclosure requirements, in the payment card industry. The table below poses the questions that emerge from our analysis.

The public legal system has modified the payment card industry’s private ordering regime in several respects, while generally leaving significant portions of the regime intact and functioning outside the reach of law. Historically speaking, apart from limited federal intervention by the FTC, legislative solutions to perceived problems in the private ordering regime have come primarily from the states, reflecting a fragmented approach toward regulatory change. This perhaps suggests the federal system operating in the United States is working as a “laboratory” in which various states experiment with legislation, as Justice Brandeis suggested in his famous dissenting opinion more than 75 years ago.

176. For perspective on this issue from credit unions, many of which may be under the ten billion dollar limit, see Adam J. Levitin, Interchange Regulation: Implications for Credit Unions (2010), available at http://www.federalreserve.gov/newsevents/files/levitin_paper.pdf. Professor Levitin also suggests industry conformity as a possible response to regulations that nominally affect only larger issuers. See id. at 36.

177. See New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."). It should be noted, however, that the “experiment” at issue in Liebmann involved a state law that allowed a private firm to exclude a competitor from entering the ice business. The majority did not disagree with the principle of experimentation, but would not countenance state interference that was deemed arbitrary and unreasonable. See id. at 279–80 ("It is plain that unreasonable or arbitrary interference or restrictions cannot be saved..."
Policy issues:

- Market price effects of breaches are significant and long term.
  - Policy issues/decisions, therefore, are nontrivial.
- Is the mosaic of regulation at state and federal level hindering rather than helping develop a sound market model?
  - Are the states (and the fed) using a bolt-on, built-in, or embedded approach? Do regulations converge and empower the private ordering solution?
- Is the due process for determining requirements fair, transparent, complete?
  - Is there a due process for determining how the assessment will be conducted? (PCI DSS auditing standards).
  - Are there set assurance requirements (audit opinions)?
  - Why is the enforcement issue left under the control of the card brand owners? Are expectations of card brands consistent with each other?
- Infrastructure and participants are globally domiciled.
  - No U.S. agency has global reach.
- Certification process is embedded within the infrastructure.
  - Qualifications, certification, training of ASQs is within the domain—a conflict of interest issue.
  - Internal security assessors are trained by the PCI SSC—an independence issue.
  - Only QSAs have the accommodation to have PCI Forensic Investigators (PFI).
- Pace of change in technology and its use is significant.
  - Is the council moving fast enough? Is the direction of development consistent with technology change? Are SIGs currently identified enough?
  - Can appropriate revisions in the law be expected to occur in a timely manner consistent with the dynamically changing technology, which affects the core requirements intended as solutions?

As Justice Brandeis also noted in that same dissenting opinion, whether legislation is effective to achieve the purposes for which it is enacted, or whether it reflects sound economic principles, are matters that are supposed to be left to the discretion of the legislature:

> Whether the enactment is wise or unwise, whether it is based on sound economic theory, whether it is the best means to achieve the desired result, whether, in short, the legislative discretion within its prescribed limits should be exercised in a particular manner, are matters for the judgment of the legislature, and the earnest conflict

from the condemnation of [the Due Process clause of the Fourteenth Amendment] merely by calling them experimental.

\)
of serious opinion does not suffice to bring them within the range of judicial cognizance.\textsuperscript{178}

Unfortunately, legislative incursions on private ordering are often motivated by politics, which does not always reflect sound economic analysis. For example, cost-benefit studies of various regulatory efforts aimed at achieving measures of public safety have vast differences in their cost-effectiveness, ranging from seatbelt and airbag requirements in automobiles (less than $150,000 per life saved) to hazardous waste listings from certain wood-preserving chemicals (nearly $10 billion per life saved).\textsuperscript{179} In the matter of air transportation, a requirement of hardened cockpit doors costs only $800,000 per life saved, while the Federal Air Marshal program may cost as much as $180 million per life saved.\textsuperscript{180} Psychological and political aspects of risk perception are the likely explanations for these varying resource allocations, which are not based on any coherent standard about acceptable levels of risk.\textsuperscript{181}

Anecdotal evidence concerning data security legislation described above suggests that legislative reactions have occurred in response to notorious cases involving security breaches, which therefore precipitate political interest in formulating a response.\textsuperscript{182} As previously discussed, some of these responses have been useful in formulating new approaches to adjust market incentives, including state disclosure laws. A single federal standard for disclosure of security breaches may well achieve a better result than a patchwork of state laws governing these responsibilities, but this may not sit well with the state political actors who seek to protect their authority to protect citizens within their jurisdictions.\textsuperscript{183} Fine tuning breach disclosure require-

\textsuperscript{178} See id. at 285 (quoting Chicago, Burlington & Quincy R. Co. v. McGuire, 219 U.S. 549, 569 (1911)).


\textsuperscript{180} See id. at 143.

\textsuperscript{181} See id. at 145–46. Stewart & Mueller suggest that an emerging benchmark for saving a life ranges from $1 to $10 million. See id. at 143. Of course, allegations of protective efforts producing costly outcomes are not limited to regulation aimed at lifesaving. See, e.g., David S. Evans & Joshua D. Wright, The Effect of the Consumer Financial Protection Agency Act of 2009 on Consumer Credit, 22 LOY. CONSUMER L. REV. 277 (2010) (critiquing the likely outcome of enhanced financial regulation as making credit more expensive and difficult to obtain, substituting the choices of bureaucrats over consumers, and jeopardizing the financial recovery).

\textsuperscript{182} See, e.g., Regan, supra note 83, at 1105–12 (highlighting various breaches giving rise to federal bills involving data security); Winn, supra note 73, at 1142–44 (discussing history of California’s security breach notification law).

\textsuperscript{183} See Regan, supra note 83 at 1120–21 (summarizing political views of those who champion states’ rights and preservation of localized authority over consumer protection issues).
ments to displace individual notification requirements would likely enhance consumer welfare on account of significant cost savings, but this is fraught with political difficulty due to the appearance of letting a breaching firm off more easily than under current law.

Statutes designed to reallocate costs from breaching merchants to issuing banks seem to present the risk that legislatures will reallocate costs within the system based on their political preferences. By creating a new path toward cost reallocation associated with payment card reissuance, there may be some marginal impact on security behavior by merchants on account of the liability threat. However, not all merchants will be able to bear those costs as effectively as the issuing banks, which have significant fee bases from a broad range of customers. Moreover, as discussed above, large transaction costs are likely in litigation, making consumer welfare enhancement unlikely. To the extent that payment networks require cost reallocations as a matter of private ordering, they are likely to take into account the business realities in this environment, particularly when other payment forms are constantly evolving to challenge the existing regime.

Although security is often a public good that is paid for by public funds, which cover police and other law enforcement protections, private firms also incur significant costs to guard against threats posed by criminal elements. Security costs to implement PCI DSS are significant, entailing fixed costs for a security infrastructure as well as ongoing expenditures to maintain and monitor compliance. Large firms with broad transaction bases are likely to have an advantage over their small business counterparts in terms of their ability to support these expenditures for security. However, small businesses are very vulnerable to security threats, and they frequently lack the resources to address them. Technology may provide new solutions in a cost-effective manner, but until those solutions emerge, a differential risk environment is likely to exist.


185. See Part III(C).

This disparity between small and large businesses creates a particularly difficult problem for legislators and regulators to resolve in seeking to intervene in the private ordering regime. Currently, the industry appears to be effectively exempting smaller businesses from more rigorous compliance burdens applicable to larger firms at the merchant level. This choice makes sense if one adopts the policy goal of trying to secure the greatest number of transactions in the most cost-effective way, while at the same time preserving the social benefits of maximizing accessibility and use of payment cards in a broad range of businesses. However, it will prove unsatisfying to those who see security as an important consumer right, akin to privacy. Those who prefer a larger federal role in shaping data security practices must recognize that enforcing additional security protections will likely have economic and social consequences, which deserve careful consideration. Before displacing the private ordering regime, legislators and regulators should have clear answers concerning the likely impacts from their efforts to ensure that implementing their good intentions does not raise consumer costs and restrict consumer access to their preferred payment mechanisms.